Cybersecurity as a global business issue
Digitalization not only calls for a transformation of business models, but also for a change in mindset for handling cybersecurity issues at companies. Taking action to protect companies against cyberattacks can only work on a global level and in cooperation with scientists, political leaders and the business community.

Since 2006, the Center for Strategic and International Studies in Washington, DC, has been recording significant cyber incidents directed toward government agencies, defense and high tech companies and economic crimes with losses of more than $1 million. The Center’s compilation briefly describes every attack or incident and the affected institution. The current document has reached 40 pages with over 300 listed incidents. Clearly, the need for companies and institutions to discuss cybersecurity on all levels cannot be denied. Every day, we can learn about new cyber incidents because criminals have substantially professionalized their tools and methods over the years.

There are countless examples of cyberattacks on companies in the US and Germany over the last decade — attacks with the potential to both affect companies as a whole as well as their supply chains and customers. “Cybersecurity is not only a question of technology or compliance, but a question of the company’s overall strategy,” points out Peter Wirnsperger, Partner and Head of the area Cyber Risk at Deloitte. He also observes that it has only been in the last couple of years that cybersecurity strategies are not just centered on IT but are also being discussed in the entire business context. “Our economy has changed so far that we have new types of companies, such as online shops, with totally different cybersecurity needs,” Wirnsperger points out. And cybersecurity plays a significant role not only for e-commerce: every company has to answer the same questions: How can we secure our market position and how can we securely implement new technology?

Cooperation between business and politics

The same also applies to government agencies and the public sector. “Safeguarding security in cyberspace and protecting critical information infrastructure are vital concerns of the 21st century and
require a high level of government commitment,” says Arne Schönbohm, President of the German Federal Office for Information Security (BSI). He explains that the German government has done more in terms of strategic development, legislation and practical measures for IT and cybersecurity over the last few years than ever before. These measures include, for example, implementing the IT Security Act in 2015 and developing a new cybersecurity strategy for Germany in 2016.

The “Cyber Security Report 2019” from Deloitte also underlines the belief that government policies can help to increase cybersecurity for companies. But two-thirds of the surveyed companies’ representatives do not consider the needs of businesses are being effectively addressed by federal government institutions. On the other hand, half of the interviewed politicians do not feel they are well informed about the problems and needs of the business world in terms of IT security. Therefore, a dialogue between politicians and companies is key to developing cybersecurity solutions.

Communicating cybersecurity on all levels

Making a distinction between the state and federal levels in Germany is also necessary for understanding cybersecurity challenges in a broader and ultimately global context. “Companies and governments are well advised to foster an open and collaborative environment in which they can freely exchange and discuss their challenges as well as lessons learned,” says Wirnsperger from Deloitte. “While such issues are not always easy and entirely pleasant to discuss openly, pursuing cross-border collaboration in open ecosystems works to the greater benefit of all.”

Cooperation between companies and the government is not only a key aspect to finding new solutions in cybersecurity, scientists and their research in this field

Facts about ransomware: A troubling evolution

Ransomware can be debilitating for businesses, negatively affecting the organization’s productivity, financial performance and brand. Malicious software denies access to a system or to data until a set amount of ransom is paid. Ransomware can enter a company’s systems through contact with an infected website or as a result of a successful phishing email. In many cases, malicious actors infiltrate a company’s systems long before they deploy the ransomware. Once they’ve gained access, these actors will then take the time to perform reconnaissance on the company’s IT infrastructure to ensure their deployed ransomware is targeted to maximize the encryption of data. Once a company’s systems are breached, the malicious actors can encrypt them and exfiltrate key files. They will then demand a ransom payment, generally in bitcoins, in exchange for the decryption key or restoration of the stolen files.

A common misperception is that malicious actors, using ransomware, target larger corporations and businesses. In fact, malicious actors, leveraging automated software and other capabilities, target organizations of all sizes from many different sectors, including state municipalities, healthcare entities and law firms. The evolution of ransomware is troubling, and ransomware attacks are on the rise:

- Conservative estimates indicate that the number of ransomware modifications is more than double the number of new samples detected during the same period last year.
- In 2019, every 14 seconds an organization falls victim to ransomware.
- A total of 1.5 million new phishing sites are created every month.

After an infection, a company faces an average downtime of 9.6 days and has to pay about $36,295, whereby the significantly higher downtime costs are not yet included here.

Source: Squire Patton Boggs

Learn more about Germany’s measures for cybersecurity in an interview with Arne Schönbohm on pp. 18–19.

Achieving greater cyber resilience as a society and within organizations will require a more concerted effort to uncover and manage new risks inherent in emerging technologies. Organizations must have the right leadership and processes in place to drive the security measures required by digital advancements. Many businesses are just beginning this journey: Relatively few respondents (34%) say their organizations plan to assess internet of things (IoT) security risks across the business ecosystem. A total of 29% of respondents say chief information security officers (CISOs) bear responsibility for IoT security.

Twenty-nine percent of respondents say CISO bear responsibility for the internet of things (IoT) security.

CISO: 29%

Engineering: 19%

Chief risk officer: 17%

Source: www.pwc.com — Strengthening digital society against cyber shocks

Source: Squire Patton Boggs
HOW BUSINESSES CAN BUILD THE RESILIENCE NEEDED TO WITHSTAND DISRUPTIVE CYBER-ATTACKS

In the 2018 Global State of Information Security® Survey (GSISS), 40% of survey respondents from organizations using robotics or automation say the disruption of operations would be the most critical consequence of a cyberattack on those systems. Despite an awareness of disruptive cyber risks, companies often remain unprepared to deal with them. Less than half of survey respondents have adopted many of the key processes for uncovering cyber risk in business.

Also need to be included. “On a scientific level, there has always been a good academic partnership between the US and Europe,” says Udo Helmbrecht, Honorary Professor at the Institute for Technological Computer Science at the Bundeswehr University in Munich. “Germany is internationally well positioned when it comes to research, patents and start-ups in cybersecurity, but they do not scale.” Often, American companies are more successful. Thus, Europe should be aware that demand also exists for it to develop new technology and business models in the field of cybersecurity. And this can only work when cooperating on a global level. “The interest in cybersecurity is equally important for all countries,” Helmbrecht says. “Therefore, we need a mutual understanding of the regulatory framework and no isolated, national solutions.”

The increasing number of cyberattacks on both companies and public institutions make it clear that solutions to prevent cybercrime can only be successful on a global level when all stakeholders work together. Additionally, businesses should support a change in mindset that recognizes cybersecurity is a topic not only handled by the IT department but within the entire company.

CENTURYLINK PROVIDES NETWORK-BASED LAYERS OF PROTECTION TO HELP BUSINESSES DEFEND AGAINST AN INCREASINGLY COMPLICATED THREAT LANDSCAPE. THE COMPANY HAS ONE OF THE LARGEST AND MOST DEEPLY PEERED IP BACKBONES IN THE WORLD, GIVING EXPANSIVE, NEAR-REAL-TIME VISIBILITY INTO THE THREAT LANDSCAPE.

Be bold — but beware: Talking about cyberthreats

Cyberthreats are escalating faster than many firms can identify, block and mitigate them. Visibility into the threat landscape is imperative, but it’s even more essential to act.

What can companies do to protect their businesses against current and future threats? Here are five recommendations:

- **Embed security into the network.** The volume and velocity of network data will continue to skyrocket. Deploying better security at a network layer will help to provide a disproportional benefit due to the increased bandwidth that video, IoT, mobile and 5G will bring.
- **Double down on the experts.** Security talent is scarce. Organizations must determine what is essential for them to architect and deliver internally and what can best be delivered by trusted partners.
- **Make security simple.** When evaluating security solutions, always consider if they improve your security, decrease your cost and reduce friction. Choose a solution that meets at least two of these criteria.
- **Close the security and engineering gap.** Security bolted onto the network later in the process can be disruptive to both the business and the user experience. It is essential that security be built into every product and solution as part of one engineering process.
- **Change how we trust.** The days of implicit trust are over. A connected device tied to a person’s identity cannot be trusted. It’s critical to look at applying security consistently across any devices associated with a person’s identity.

Ralf Straßberger
Managing Director Germany, Austria & Switzerland, CenturyLink
www.centurylink.com